Communications Security Establishment Commissioner

Annual Report

2005-2006

Canada

Office of the Communications Security Establishment Commissioner
P.O. Box 1984
Station "B"
Ottawa, Ontario
K1P 5R5

Tel.: (613) 992-3044
Fax: (613) 992-4096
Website: http://csec-ccst.gc.ca

© Minister of Public Works and Government Services Canada 2006
ISBN 0-662-49258-7
Cat. No. D95-2006

Communications Security
Establishment Commissioner

The Right Honourable Antonio Lamer,
P.C., C.C., C.D., LL.D., D.U.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

Le très honorable Antonio Lamer,
c.p., C.C., c.d., LL.D., d.u.

April 2006

Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Sir:

Pursuant to subsection 273.63 (3) of the *National Defence Act*, I am pleased to submit to you my 2005–2006 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

Antonio Lamer

P.O. Box/C.P. 1984, Station "B"/Succursale « B »
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

TABLE OF CONTENTS

The Commissioner's Role 1

The Review Environment 3

- Three-year review of the Anti-Terrorism Act 3
- "Whistle-blower" legislation 4
- Bills that died on the order paper 4
- The Arar Commission 6
- Interception of private communications by the U.S. National Security Agency 7

The Year in Review 8

- Review activities and highlights 8
  - Workplan 8
  - Methodology 8
  - Reviews undertaken 9
  - Legal interpretations 9
  - Review highlights 10
- 2005–2006 findings 11
- Complaints about CSE activities 12
- Duties under the Security of Information Act 12

The Impact of Review 12

The Commissioner's Office 14

Looking to the Future 15

- Internationally 15
- At home 15

In Closing 17

Annex A: Mandate of the Communications Security Establishment Commissioner 19

Annex B: Classified Reports, 1996–2006 21

Annex C: Statement of Expenditures, 2005–2006 25

Annex D: History of the Office of the Communications Security Establishment Commissioner (OCSEC) 27

THE COMMISSIONER'S ROLE

Parliament passed the *Anti-Terrorism Act* in December 2001. This amended the *National Defence Act* (*NDA*) and established in legislation the role and responsibilities of the Communications Security Establishment (CSE) and the CSE Commissioner.

My primary legislated duty is to review the activities of CSE to determine whether they comply with the laws of Canada. The Act charges me to review CSE's activities in general and, as well, specifically to review activities that CSE carries out under ministerial authorization. Given the nature of CSE's activities, I place a particular emphasis on determining whether those activities are carried out in a manner that appropriately protects the privacy of Canadians,[1] as CSE is required to do by law.

My other duties include undertaking such investigations as I consider necessary in response to any complaints received about CSE's activities, and informing the Minister of National Defence and the Attorney General of Canada about any CSE activity that I believe may not be in compliance with the law.

As I see it, my main role as the CSE Commissioner is to give assurance to the Minister of National Defence that the intrusive powers Parliament granted to CSE are used in accordance with the legislation. Annex A of this report sets out the key elements of my mandate under the *National Defence Act*, as well as my duties under the *Security of Information Act*.

The Communications Security Establishment, the subject of my attention as Commissioner, is a central player in Canada's security and intelligence community. CSE's mandate under Part V.1 of the *National Defence Act* includes:

- acquiring and using information from the global information infrastructure to provide the

[1] It is important to note that "Canadians" includes Canadian citizens, permanent residents and corporations incorporated in Canada.

Government of Canada with foreign intelligence[2] in accordance with the government's intelligence priorities;

- helping to protect electronic information and information infrastructures that are of importance to the Government of Canada; and
- providing technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

I carry out all my responsibilities in full recognition of the importance of CSE's contribution to ensuring that the Government of Canada is in a position to play an active, well-informed role in promoting and protecting Canadian interests in a rapidly changing world. In light of the continuing threat of terrorism around the world in recent years, I am particularly aware of CSE's important contribution to protecting the security of Canada and Canadians. It is not my intention to impede CSE from fulfilling its important role. Rather, I believe that CSE's effectiveness is enhanced when I am able to provide evidence-based assurance not only about the lawfulness of its activities, but also about the policies, procedures and processes it has in place to help ensure that lawfulness.

I am pleased to submit this annual report summarizing my office's activities and findings for the year ended 31 March 2006. In doing so, I would like to express my appreciation for the cooperation and assistance that my office received from the CSE's new Chief and his staff throughout the year. Although it is normal, and indeed fitting, for a measure of healthy tension to exist in the relationship between any review body and the organization being reviewed, the professionalism of CSE's employees

[2] Foreign intelligence is defined in Part V.1 of the *NDA* as "information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security".

has facilitated the work of my office and made it more productive.

THE REVIEW ENVIRONMENT

Several developments during the year, some of them new and some of them continuing, have the potential to shape the security and intelligence sector in general, as well as the roles and responsibilities of review bodies such as my office. I have monitored these developments closely and seized the opportunity to contribute to them as appropriate.

Three-year review of the Anti-Terrorism Act

The omnibus *Anti-Terrorism Act* resulted in key amendments to several existing Acts, including amendments to the *National Defence Act* that provided the legislative basis for CSE as well as the CSE Commissioner. The *Anti-Terrorism Act* required a review of its provisions and operation within three years of receiving Royal Assent, and the Special Senate Committee on the *Anti-Terrorism Act* was created for this purpose in December 2004.

I appeared before the Special Senate Committee on 13 June 2005, as well as the House of Commons Sub-Committee on Public Safety and National Security two days later, on 15 June. On both occasions, I set out my views on the legislation, based on the experience of this office since its enactment. In my remarks, I made it very clear that the legislation itself is absolutely essential. However, I noted also that fine-tuning and clarification of some of its provisions — particularly those relating to ministerial authorizations to intercept private communications for the purpose of obtaining foreign intelligence[3] — would help eliminate ambiguities and ensure a common understanding of the operational application of these provisions. In

[3] In my 2004–2005 Annual Report, I outlined my views in some detail on how I have interpreted and will continue to discharge my mandate in respect of foreign intelligence ministerial authorizations (pp. 7-10).

addition to my appearances, I wrote to the Chair of the Sub-Committee to provide my views on certain recommendations made by other witnesses that would affect my office.

Upon the dissolution of Parliament in November 2005, the Special Senate Committee on the *Anti-Terrorism Act* was also dissolved without having issued its report. The new Parliament was not yet in session when my reporting period ended on 31 March 2006, but I will monitor future developments in this area with keen interest.

"Whistle-blower" legislation

The *Public Servants Disclosure Protection Act* (the so-called "whistle-blower" legislation) received Royal Assent in November 2005. The Act establishes procedures for the disclosure of wrongdoings in the public sector and provides for the protection of persons who disclose the wrongdoings. Although my office will be subject to this Act, the Communications Security Establishment is excluded from the definition of "public sector" and thus from its general application. However, the Act provides that excluded organizations, such as CSE, must establish similar procedures, specific to the organization concerned.

The Act has yet to come into effect, and I understand that Bill C-2 (*Federal Accountability Act*) tabled by the new government may change some of the provisions of the "whistle-blower" legislation. Nevertheless, it is probable that CSE will be required to establish procedures for the disclosure of wrongdoings, including the protection of persons who disclose them — with a possible review role for the CSE Commissioner. I am quite prepared to take on responsibilities in this regard if called upon to do so.

Bills that died on the order paper

Two proposed pieces of legislation with the potential to influence the environment within which my office carries out its work died on the order paper when Parliament was dissolved in November 2005. As of

the end of this reporting period, the new government had not yet announced whether either initiative will be pursued.

Bill C-74 (*Modernization of Investigative Techniques Act*) received first reading in the House of Commons in November 2005. The Bill would require telecommunications service providers to put in place and maintain capabilities that facilitate the lawful interception of information transmitted by telecommunications, and to provide basic information about their subscribers to specified authorities.

The proposed legislation would not affect CSE's mandate in relation to foreign intelligence or its mandate to protect electronic information and information infrastructures. It could, however, influence the extent of the technical and operational assistance CSE provides to federal law enforcement and security agencies in the performance of their lawful duties.

Bill C-81 (*An Act to establish a National Security Committee of Parliamentarians*) also received first reading in the House of Commons in November 2005. The mandate of the proposed committee would be to review the legislative, regulatory, policy and administrative framework for national security, and the activities of federal departments and agencies relating to national security. It is not intended, however, to duplicate the work of existing review bodies.

I would welcome the prospect of Parliament playing a more active role in security and intelligence matters, including scrutiny of the work of review bodies such as my office. However, I also recognize some challenges in this regard. These include, for example, the composition of the committee and its access to classified information and documents.

The Arar Commission

The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, chaired by Mr. Justice Dennis O'Connor, was established in February 2004. Among other things, the Commission is mandated to recommend a review mechanism for the activities of the Royal Canadian Mounted Police (RCMP) with respect to their national security activities. In relation to this part of its mandate, the Commission examined intelligence review models in Canada and internationally, and held public consultations. My office contributed both written and oral submissions. My basic message to the Commission was that the model already in place for reviewing Canada's security and intelligence agencies is a good one, and experience shows that it works.

The key characteristics of the model include separate review agencies, with each review agency having:

- a mandate aligned specifically to the functions and activities of the agency reviewed;
- full independence;
- broad, unfettered access to facilities, personnel and information;
- authority to review all operational activities as well as to investigate complaints; and
- the responsibility to report to the minister accountable to Parliament for the agency under review, so that accountability to Parliament is clear and uncompromised.

The strengths of the model, therefore, include appropriateness, effectiveness and accountability. Moreover, the model's flexibility means that it can be readily adapted to particular circumstances and requirements, including a mechanism uniquely suited to reviewing the RCMP's national security activities.

I look forward with interest to the Commission's report and its recommendations.

Interception of private communications by the U.S. National Security Agency

In late 2005, the United States media reported that following the events of 11 September 2001, President George W. Bush ordered the National Security Agency (NSA), in the interests of national security, to intercept private communications of Americans without a court warrant. In doing so, according to press reports, the President bypassed the process established for such circumstances under the *Foreign Intelligence Surveillance Act* of 1978.

Understandably, questions, commentary and speculation began to appear in the Canadian media about CSE's role and activities in the current threat environment. As a result, I made my own extensive inquiries that included discussions and communications with the Chief, CSE and drew on the considerable body of work carried out by my office in recent years. It is not my intention to comment in any way on the lawfulness of the NSA's activities, as they are well beyond my purview. However, I have decided to take the opportunity afforded me by this Annual Report to highlight the regime in place in Canada.

Part V.1 of the *National Defence Act* allows CSE to collect communications, even if they enter or exit Canada, provided that the target for the collection is a foreign entity located outside of Canada. In other words, the target cannot be a Canadian or located geographically in Canada. This kind of collection, where the end not targeted is in Canada, must be authorized by the Minister of National Defence in advance of the collection. The *NDA* sets out conditions that must be met to the Minister's satisfaction in order for a ministerial authorization to be issued. It was Parliament's view that a ministerial authorization, entrenched in legislation, provides a better approach to establishing the required authority

than a court warrant, as the latter would have no application to foreign targets located outside Canada.

The regime in place for CSE to acquire communications of foreign entities, even if a communication originates in or enters Canada (and is thus a private communication[4]), is based in legislation. Further, the *NDA* requires me, as the CSE Commissioner, to review CSE activities to ensure that they comply with the law. It directs me specifically to review activities carried out under a ministerial authorization to ensure they were authorized, and to report annually to the Minister on my review. A summary of my review work completed in the year ended 31 March 2006 follows.

THE YEAR IN REVIEW

Review activities and highlights

Workplan

A regularly updated three-year workplan guides my office's review program. This plan, which I approve, is driven in part by my staff's extensive knowledge of CSE's activities. It gives priority to reviewing those activities where the risks to the privacy of Canadians are believed highest.

Methodology

My staff has access to all the CSE premises, documents, files and personnel required to carry out reviews. They conduct thorough file and document reviews, interview CSE officials and carry out a variety of checks and tests to determine whether CSE has carried out its activities lawfully and has appropriately protected the privacy of Canadians. It is important to note that these reviews are normally carried out after the fact, in order not to intervene, without cause, in CSE's activities and operations while they are being conducted.

[4] The *Criminal Code* definition of a private communication includes any communication that originates or terminates in Canada made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended.

When a review is completed, I provide a classified report to the Minister of National Defence.[5] Each report provides the Minister with my opinion on the lawfulness of the activities reviewed and includes any recommendations that I consider to be appropriate in the circumstances. Such recommendations generally address shortcomings in CSE's policies, procedures or practices that, if not corrected, increase the risk that unlawful activity might occur. In this, as in so many other cases, I am firmly convinced that an ounce of prevention is worth a pound of cure.

Reviews undertaken

In 2005–2006, my office completed a total of seven reviews. Six reviews were of CSE activities carried out under ministerial authorization. One of these six dealt with foreign intelligence collection, and five involved information technology security (ITS) operations. I also submitted a classified report to the Minister on a subject related to my general mandate to review the activities of CSE to ensure they are in compliance with the law. None of my seven reviews of CSE activities completed in 2005–2006 reported unlawful conduct.

Legal interpretations

With respect to my reviews of CSE activities carried out under ministerial authorization, I note that I concluded on their lawfulness in light of the Department of Justice interpretation of the applicable legislative provisions. I have pointed out elsewhere that there are ambiguities in the legislation as now drafted, a view that I share with my predecessor, the Hon. Claude Bisson, O.C., a former Chief Justice of Quebec. Currently, two eminent lawyers, the Deputy

[5] Annex B lists all classified reports produced by the CSE Commissioner since 1996, when this office was established.

Minister of Justice and my independent Legal Counsel disagree over the meaning of key provisions that influence the nature of the assurance that I can provide. This underlines the importance of seizing the next opportunity to make statutory amendments.

Review highlights

Findings from my recent reviews of foreign intelligence collection under ministerial authorization have drawn my attention to the process CSE uses to translate approved government intelligence priorities into targeting specific foreign entities. I believe it should be possible to identify a clear linkage between the government intelligence priorities, the foreign entities targeted and the activity or class of activities for which ministerial authorization is needed.

However, reviews completed by my office, including the most recent one, have shown that supporting documentation provided by CSE as part of requests for the Minister's authorization address the underlying foreign intelligence requirements only in general terms. The lack of clarity in this regard has made it difficult for my staff to assess compliance with certain of the conditions that the legislation requires to be satisfied before a ministerial authorization is given. I have offered specific recommendations to the Minister and CSE for strengthening the process.

I provided a single integrated report to the Minister on the five reviews of ITS activities carried out by CSE under ministerial authorizations. As in previous reports, I set out in this report my continuing concern with CSE's record-keeping practices. I recognize that CSE is taking steps to improve its corporate records management practices in general. The authority to intrude on the privacy of Canadians in the course of protecting the government's computer systems and networks under an ITS ministerial authorization is a sensitive matter. CSE has acknowledged its

responsibility to be able to record and account for such intrusions. I believe that CSE ought to give prompt attention to improving record-keeping practices in this regard, and I have asked my staff to monitor this issue closely in future reviews.

Under my general mandate to review the activities of CSE to ensure they comply with the law, I examined CSE's foreign intelligence collection activities directed at countering the threat posed by the proliferation of weapons of mass destruction and their delivery systems. Following the terrorist attacks in the U.S. in 2001, CSE enhanced its activities in the counter-proliferation area. It sends reports, based on the intelligence it collects and analyses, to Government of Canada clients and to allied agencies.

In June 2005 I provided the Minister with a classified report setting out the findings of this review. The CSE activities I reviewed complied with the law. The review identified, however, areas of policy weakness and, in one instance, a need to reconcile policy and practice. CSE accepted my recommendations, though in some cases with modifications, which they explained to me.

2005–2006 findings

In accordance with well-established practice, in each Annual Report I summarize my findings about the lawfulness of CSE's activities based on the reviews my office has completed in the past year. I am able to report that the CSE activities examined during the period under review complied with the law as it is currently interpreted by the Department of Justice, and I am satisfied that CSE lawfully used and retained the intercepted private communications that were examined by my office in 2005–2006.

Complaints about CSE activities

In addition to setting out my review mandate, the *National Defence Act* also requires me, in response to a complaint, to undertake any investigation I consider necessary to determine whether CSE engaged, or is engaging in unlawful activity. Complaints may be submitted by Canadians who believe that CSE has acted unlawfully in the performance of its duties. Until this past year, the Commissioner's office had received no complaints that required formal investigation.

There were again a limited number of complaints in 2005–2006 and, with one exception, they were not within my mandate. The one complaint received that both fell within my mandate and required investigation was still under investigation at the end of this reporting year. I anticipate that the investigation will be completed in spring 2006, after which I will report my findings to the Minister.

Duties under the Security of Information Act

The *Security of Information Act* establishes a process that persons permanently bound to secrecy under the Act must follow if they wish to claim a "public interest" defence for divulging classified information. For classified information about CSE, the CSE Commissioner is part of the process (see Annex A). No such matters were referred to me in 2005–2006.[6]

THE IMPACT OF REVIEW

The impact of review by an office such as mine may be direct or indirect. Assessing that impact is inherently difficult because, if effective, its main influence is on preventing unlawful or undesirable acts or things from happening.

Indirect impacts can result simply from the existence and mandate of a review body, and the effect these have on how the reviewed organization conducts its

[6] My website at **http://csec-cest.gc.ca** provides an overview of my office's processes for handling complaints under the *National Defence Act* and for concerns raised pursuant to the *Security of Information Act*.

affairs. Nevertheless, my observations and discussions over the past three years make me confident that the mandate and work of my office has a positive influence on the manner in which CSE carries out its activities and on helping to ensure that they are conducted in compliance with the law.

The findings and recommendations of specific reviews have a more direct impact — particularly as a result of the action that the reviewed organization takes in response to them. When warranted by the findings, my review reports may include recommendations for action by CSE to correct deficiencies in policies, procedures or practices that increase the risk of unlawful activity. The status of recommendations is the subject of periodic discussions between my staff and CSE, and my office continues to track their disposition.

I am encouraged by CSE's positive response to the recommendations my office has made. Of almost 100 recommendations made by the CSE Commissioner since the establishment of this office, 75 percent were accepted by CSE and have either been fully implemented or are at various stages of being implemented. Half of the remaining recommendations were accepted with some modifications or are very recent and are still being considered by CSE. The remainder were either bypassed by events or, in a few cases, not accepted by CSE. Where CSE has either accepted recommendations with modifications or has rejected them, CSE officials have explained the reasons to me, with some discussions still pending.

I commend the new Chief of CSE for his ready acceptance of the importance of review, and welcome his continuing cooperation and willingness to help my office monitor the status of recommendations as an important indicator of the impact of review.

THE COMMISSIONER'S OFFICE

In 2005–2006, my office's expenditures of $1,043,540 were well within budget for the period. Annex C to this report provides a summary of 2005–2006 expenditures.

In carrying out my mandated responsibilities, I continue to rely on the expertise, loyalty and commitment of my staff. My office has a full-time working staff of eight people, supplemented by contracted professionals who bring a range of skills, knowledge and experience to bear as and when required.

I encourage and support several activities to help ensure that my staff continues to sharpen skills, broaden knowledge and experience, and remain fully engaged in the review community and in issues facing the security and intelligence sector in general. Such developmental opportunities in 2005–2006 included:

- initiating what has become known as the Review Agencies Forum. This involves my staff as well as the staffs of the Security Intelligence Review Committee, the Office of the Inspector General of the Canadian Security Intelligence Service and the Commission for Public Complaints Against the RCMP, who meet and share experiences, discuss issues of mutual interest and concern and identify best practices in review;
- continuing to host informal presentations to my office by government officials and academics on matters relating to security and intelligence as well as review;
- attendance of my staff at several conferences and symposia, including the 20th Anniversary International Conference of the Canadian Association for Security and Intelligence Studies; an International Symposium on Making National Security Accountable; the National Security

Studies Seminar of the Canadian Forces College; and the 4th Annual Charter Conference of the Ontario Bar Association.

In 2004–2005, my staff began the practice of giving presentations to new CSE employees — as part of their orientation course — about the duties, powers and work of the CSE Commissioner. These presentations continued in 2005–2006. I believe that this is an excellent way for my office to participate in assuring that CSE employees are aware of the Commissioner's mandate as well as how this mandate is discharged in practice.

LOOKING TO THE FUTURE

Internationally

Since assuming my responsibilities as the CSE Commissioner almost three years ago, terrorism has continued to be a dominant issue on the international political and security scene. Since my last report, the global war on terrorism has continued unabated. There have been numerous attacks around the globe, including the bombings in London, England in July 2005 and the subsequent arrest of alleged terrorists. International concerns have also increased sharply over the proliferation of weapons of mass destruction, with a particular focus on North Korea and the nuclear ambitions and intentions of Iran.

In Afghanistan, Canada accepted a lead role in providing security and helping to re-build the area in and around Kandahar. This undertaking has been made all the more important and dangerous with Osama bin Laden's exhortation to his extremist followers to prepare for a protracted war with the West.

At home

In Canada, terrorism, the proliferation of weapons of mass destruction and military deployments are not our only concerns. Canada is an integral part of an economically interdependent world and must

continue both to protect and promote its national interests in that context.

With no foreseeable diminution in perceived threats to the security of Canada and Canadians, or of the need to provide the Government of Canada with the foreign intelligence it requires to pursue and to protect Canada's interests around the world, CSE's role will continue to be important. By extension, I believe that the work of my office in reviewing CSE's activities, in assessing their compliance with the law, and in making recommendations to ensure that such compliance is based on sound policies, procedures and practices, has a useful role to play.

Many government initiatives and activities do not fit neatly into the artificial construct of a particular fiscal year. As a result, there are several matters that will carry forward, and that I hope to see completed or otherwise resolved early in 2006–2007. These include, for example, the three-year review of the *Anti-Terrorism Act*, the Bills that died on the order paper when the 38th Parliament was dissolved, and the report of the Arar Commission, as discussed earlier in this report.

In terms of the work of my office, a major, two-phased review of CSE's activities in support of the RCMP is nearing completion. My 2004–2005 Annual Report included a general outline of the Phase 1 findings and recommendations. I am hopeful that outstanding issues arising from the Phase 2 work will be expeditiously resolved, and I plan to report the Phase 2 findings and recommendations to the Minister early in 2006–2007.

Finally, to ensure that the watcher is indeed watched, I have recently commissioned two independent management reviews of my own office. One will focus on administration, including the management and control of financial, human and information

resources. The other will deal with operations, by assessing whether the office carries out the Commissioner's mandated responsibilities efficiently and effectively. The reviews will address those aspects of administration and operations that pose potential risks for this office and that are important to get right. As such, I expect that they will provide evidence-based assurance in relation to some matters, as well as recommendations for action where improvements are necessary. Both reviews are scheduled to be completed in summer 2006.

IN CLOSING

My term expires on 19 June 2006. As a result, this is my last report as CSE Commissioner. I must say that I am extremely grateful for the opportunity I have had to serve Canada, this country that I love, in a capacity that has brought its challenges, but that I have found to be rewarding in so many different ways. My one regret will be if I leave this position without a resolution of the legal interpretation issues that have bedevilled this office since December 2001. If that does indeed turn out to be the case, I wish my successor well in bringing this matter to a satisfactory conclusion for all concerned.

Mandate of the Communications Security Establishment Commissioner

National Defence Act – Part V.1

273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

(2) The duties of the Commissioner are

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

[...]

273.65 (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

Security of Information Act

15. (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]

(5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]

(b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

Classified Reports, 1996–2006

1. Classified Report to the Minister
   – March 3, 1997 (TOP SECRET)

2. Classified Report to the Minister
   – Operational policies with lawfulness implications – February 6, 1998 (SECRET)

3. Classified Report to the Minister
   – CSE's activities under *** – March 5, 1998 (TOP SECRET Codeword/CEO)

4. Classified Report to the Minister
   – Internal investigations and complaints – March 10, 1998 (SECRET)

5. Classified Report to the Minister
   – CSE's activities under *** – December 10, 1998 (TOP SECRET/CEO)

6. Classified Report to the Minister
   – On controlling communications security (COMSEC) material – May 6, 1999 (TOP SECRET)

7. Classified Report to the Minister
   – How we test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) – June 14, 1999 (TOP SECRET Codeword/CEO)

8. Classified Report to the Minister
   – A study of the *** collection program – November 19, 1999 (TOP SECRET Codeword/CEO)

9. Classified Report to the Minister
   – On *** – December 8, 1999 (TOP SECRET/COMINT)

10. Classified Report to the Minister
    – A study of CSE's *** reporting process — an overview (Phase I) – December 8, 1999 (SECRET/CEO)

11. Classified Report to the Minister
    – A study of selection and *** — an overview – May 10, 2000 (TOP SECRET/CEO)

12. Classified Report to the Minister
– CSE's operational support activities under *** — follow-up – May 10, 2000 (TOP SECRET/CEO)

13. Classified Report to the Minister
– Internal investigations and complaints — follow-up – May 10, 2000 (SECRET)

14. Classified Report to the Minister
– On findings of an external review of CSE's ITS program – June 15, 2000 (SECRET)

15. Classified Report to the Minister
– CSE's policy system review – September 13, 2000 (TOP SECRET/CEO)

16. Classified Report to the Minister
– A study of the *** reporting process — *** (Phase II) – April 6, 2001 (SECRET/CEO)

17. Classified Report to the Minister
– A study of the *** reporting process — *** (Phase III) – April 6, 2001 (SECRET/CEO)

18. Classified Report to the Minister
– CSE's participation *** – August 20, 2001 (TOP SECRET/CEO)

19. Classified Report to the Minister
– CSE's support to ***, as authorized by *** and code-named ***
– August 20, 2001 (TOP SECRET/CEO)

20. Classified Report to the Minister
– A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – August 21, 2002 (SECRET)

21. Classified Report to the Minister
– CSE's support to ***, as authorized by *** and code-named *** – November 13, 2002 (TOP SECRET/CEO)

22. Classified Report to the Minister
– CSE's *** activities carried out under the *** 2002 *** Ministerial authorization – November 27, 2002 (TOP SECRET/CEO)

23. Classified Report to the Minister
– Lexicon of CSE definitions – March 26, 2003 (TOP SECRET)

24. Classified Report to the Minister
– CSE's activities pursuant to *** Ministerial authorizations including ***
– May 20, 2003 (SECRET)

25. Classified Report to the Minister
– CSE's support to ***, as authorized by *** and code-named *** — Part I
– November 6, 2003 (TOP SECRET/COMINT/CEO)

26. Classified Report to the Minister
– CSE's support to ***, as authorized by *** and code-named *** — Part II
– March 15, 2004 (TOP SECRET/COMINT/CEO)

27. Classified Report to the Minister
– A review of CSE's activities conducted under *** Ministerial authorization
– March 19, 2004 (SECRET/CEO)

28. Classified Report to the Minister
– Internal investigations and complaints — follow-up – March 25, 2004
(TOP SECRET/CEO)

29. Classified Report to the Minister
– A review of CSE's activities conducted under 2002 *** Ministerial
authorization – April 19, 2004 (SECRET/CEO)

30. Classified Report to the Minister
– Review of CSE *** operations under Ministerial authorization – June 1, 2004
(TOP SECRET/COMINT)

31. Classified Report to the Minister
– CSE's support to *** – January 7, 2005 (TOP SECRET/COMINT/CEO)

32. Classified Report to the Minister
– External review of CSE's *** activities conducted under Ministerial
authorization – February 28, 2005 (TOP SECRET/COMINT/CEO)

33. Classified Report to the Minister
– A study of the *** collection program – March 15, 2005
(TOP SECRET/COMINT/CEO)

34. Classified Report to the Minister
– Report on the activities of CSE's *** – June 22, 2005 (TOP SECRET)

35. Classified Report to the Minister
– Interim report on CSE's *** operations conducted under Ministerial authorization – March 2, 2006 (TOP SECRET/COMINT)

36. Classified Report to the Minister
– External review of CSE *** activities conducted under Ministerial authorization – March 29, 2006 (TOP SECRET/CEO)

Statement of Expenditures 2005–2006

Standard Object Summary

Salaries and Wages	$527,760
Transportation and Telecommunications	16,655
Information	24,177
Professional and Special Services	321,484
Rentals	132,326
Purchased Repair and Maintenance	426
Materials and Supplies	7,155
Acquisition of Machinery and Equipment	9,591
Other Expenditures	3,966
Total	**$1,043,540**

History of the Office of the Communications Security Establishment Commissioner (OCSEC)

The Office of the Communications Security Establishment Commissioner was created on June 19, 1996, with the appointment of the inaugural Commissioner, The Honourable Claude Bisson, O.C., a former Chief Justice of Quebec, who held the position until June 2003. He was succeeded by the Right Honourable Antonio Lamer, P.C., C.C., C.D., LL.D., D.U., Chief Justice of Canada (retired) for a term of three years.

For the first six years (from June 1996 to December 2001), the Commissioner carried out his duties under the authority of Orders in Council issued pursuant to Part II of the *Inquiries Act*. During this period, the Commissioner's responsibilities were twofold: to review the activities of the Communications Security Establishment (CSE) to determine whether they conformed with the laws of Canada; and to receive complaints about CSE's activities.

Following the terrorist attacks in the United States on September 11, 2001, Parliament adopted the omnibus *Anti-Terrorism Act* which came into force on December 24, 2001. The omnibus Act introduced amendments to the *National Defence Act*, by adding Part V.1 and creating legislative frameworks for both OCSEC and CSE. It also gave the Commissioner new responsibilities to review activities carried out by CSE under a ministerial authorization.

The omnibus legislation also introduced the *Security of Information Act* that replaced the *Official Secrets Act*. This legislation gives the Commissioner specific duties in the event that a person, who would otherwise be permanently bound to secrecy, seeks to defend the release of classified information about CSE on the grounds that it is in the public interest.

Under the Commissioner's current mandate, which entrenched in law the original mandate established in 1996 as well as the additional responsibilities described above, the Commissioner has retained the powers of a commissioner under Part II of the *Inquiries Act*.